



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



**020.308 Out-Processing/Termination of Information
Technology Personnel**



**Version 2.3
March 29, 2018**

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

Revision History

Date	Version	Description	Author
5/2/2005	1.0	Effective Date	CHFS IT Policies Team Charter
3/29/2018	2.3	Revision Date	CHFS OATS Policy Charter Team
3/29/2018	2.3	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS IT Executive (or designee)	3/29/2018	Jennifer Harp	
CHFS Chief Security Officer (or designee)	3/29/2018	DENNIS E. LEBER	

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

Table of Contents

020.308 OUT-PROCESSING/ TERMINATION OF INFORMATION TECHNOLOGY PERSONNEL.....	5
1 POLICY OVERVIEW.....	5
1.1 PURPOSE	5
1.2 SCOPE	5
1.3 MANAGEMENT COMMITMENT.....	5
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.5 COMPLIANCE	6
2 ROLES AND RESPONSIBILITIES	6
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	6
2.2 SECURITY/PRIVACY LEAD	6
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	6
2.4 CHFS STAFF AND CONTRACTOR EMPLOYEES	7
2.5 KENTUCKY ONLINE GATEWAY (KOG) ENTERPRISE IDENTITY MANAGEMENT (EIM) ADMINISTRATORS	7
2.6 SERVICE REQUESTOR	7
2.7 CHFS OFFICE OF HUMAN RESOURCE MANAGEMENT (OHRM) PERSONNEL LIAISON	7
3 POLICY REQUIREMENTS	7
3.1 GENERAL	7
3.2 STATE PERSONNEL: RESIGNATION	8
3.3 STATE PERSONNEL: SUSPENSION/ADMINISTRATIVE LEAVE.....	8
3.4 STATE PERSONNEL: TERMINATION	9
3.5 CONTRACT PERSONNEL	9
4 POLICY MAINTENANCE RESPONSIBILITY	9
5 POLICY EXCEPTIONS	10
6 POLICY REVIEW CYCLE.....	10
7 POLICY REFERENCES	10

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

Policy Definitions

- **Agency:** For the purpose of this document, agency or agencies refers to any department under the Cabinet of CHFS.
- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Personnel:** An employee hired through a state approved (i.e. SDS Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Enterprise Identity Management (EIM):** Identity management solution used to provide internal users with network service entitlements. Kentucky utilizes KHRIS and KOG to feed into the backend EIM solution.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Personnel:** An employee hired directly through the state within the CHFS.

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

020.308 Out-Processing/ Termination of Information Technology Personnel

Category: 020.300 Administrative Security

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must implement an acceptable level of security controls through an out-processing/termination policy. This document establishes the agency's Out-Processing/Termination of Information Technology (IT) Personnel Policy to manage risks and provide guidelines for security best practices regarding staff being dismissed or leaving a project/state employment.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective enacted by this policy. Violations may result in disciplinary action, which may include suspension, restricted access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

2.5 Kentucky Online Gateway (KOG) Enterprise Identity Management (EIM) Administrators

Authorized KOG personnel are responsible for taking electronically submitted service requests received by KOG and submitting them to the Commonwealth Service Desk for completion. These authorized staff personnel are responsible for basic validation of service request information and are listed as an approved IT service contact to submit service desk tickets for CHFS.

2.6 Service Requestor

A CHFS division director approved and appointed designated individual(s) to submit service requests through KOG (i.e. Active Directory (AD), Virtual Private Network (VPN), Home Folder, Shared Folder, Telephone, Enhanced Mailbox, Account, Skype for Business, Other). These designated personnel validate all KOG required user and billing code information obtained from the CHFS personnel requesting services.

2.7 CHFS Office of Human Resource Management (OHRM) Personnel Liaison

A CHFS approved and appointed designated OHRM individual(s) to submit requests through the Kentucky Human Resource Information System (KHRIS) for state CHFS staff.

3 Policy Requirements

3.1 General

This policy outlines guidelines regarding how the Cabinet for Health and Family Services (CHFS) handles departure or termination of all CHFS Information Technology (IT) employees. Contracted technical personnel, are subject to greater scrutiny apart from CHFS state employees. IT personnel have a level of access to Cabinet IT resources that require additional cautions. This policy will outline the measures to be taken when a termination notice is received.

All exit procedures for state personnel can be found on the Office of Human Resource Management (OHRM) [Exiting Employees \(for Supervisors\) Checklist](#). All IT staff must comply with this policy and all related OHRM procedures.

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

3.2 State Personnel: Resignation

When an IT state employee submits their resignation the designated OHRM personnel liaison will submit a request in Kentucky Human Resource Information System (KHRIS) for network, application, and service access to be revoked. It is the responsibility of the manager/supervisor, or designee, to follow exit procedures and determine the timeline by which the employee will transition their tasks to a successor. The applicable manager/supervisor, or designee, must determine the state owned devices/resources that must be recovered (i.e. access badge, laptop computer, keys, etc.). In case the employee is leaving state government altogether, the manager/supervisor, or designee, would confer with the second level manager/supervisor in making this determination.

If the manager/supervisor, or designee, need access to the employee's mailbox they must submit an approved/signed COT Email Review Request (COT-F084) Form to the Commonwealth Service Desk (CSD) (CommonwealthServiceDesk@ky.gov). If the manager/supervisor, or designee, need access to the employees file shares (i.e. shared folders, U: Drive, etc.) they must submit an approved Staff Service Request Form, EZ Version (COT-F181EZ) to the CSD. For any employees who have EAS Domain accounts (i.e. Developers, Admin Accounts, etc.) the manager/supervisor, or designee, must submit an approved Staff Service Request (COT-F181) Form to the CSD to terminate these accounts.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information, that could be used by departed employees to hinder an application/system.

3.3 State Personnel: Suspension/Administrative Leave

When an employee is suspended or placed on administrative leave, their network accounts must be disabled immediately during the suspension/leave period. The designated OHRM personnel liaison, must update the employee's suspension/administrative leave in KHRIS. If the manager/supervisor, or designee, need access to the employee's mailbox, file shares, or EAS Domain accounts, follow the process detailed in Section 3.2 above.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information, that could be used by departed employees to hinder an application/system.

Once the employee returns to work, the designated OHRM personnel liaison, must update the employees account in KHRIS to request the accounts be enabled. The OHRM Personnel Procedures Handbook – 4.1 Disciplinary/Corrective Action must be followed.

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

3.4 State Personnel: Termination

Should a situation arise where an employee who has merit status is being terminated and has been issued intent to dismiss letter, all access must be revoked/terminated. At the time the intent is issued, any administrative rights, as well as all other access must be removed. If the applicable supervisor deems the employee a risk to Commonwealth assets, they, or the designated service requestor, must update KHRIS to remove all rights and privileges for that employee immediately.

Once the decision has been made to terminate an employee, the applicable manager/supervisor, or designee, must determine the state owned devices/resources that must be recovered (i.e. access badge, laptop computer, keys, etc.). The terminated employee is prohibited from having any unsupervised access to the network. If it is determined that the former employee is to be allowed to recover email messages, addresses, or any personal documentation, the immediate supervisor will remain with that employee until the task is complete. If the manager/supervisor, or designee, need access to the employee's mailbox, file shares, or EAS Domain accounts, follow the process detailed in Section 3.2 above.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information, that could be used by departed employees to hinder an application/system.

3.5 Contract Personnel

When a contractor departs, their state manager/supervisor, or designated service requestor, must update the Kentucky Online Gateway (KOG) to immediately revoke all rights and privileges. Once the decision has been made to terminate a contract employee, the applicable manager/supervisor, or designee, must determine the state owned devices/resources that must be recovered (i.e. access badge, laptop computer, keys, etc.). If the manager/supervisor, or designee, need access to the employee's mailbox, file shares, or EAS Domain accounts, follow the process detailed in Section 3.2 above.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information, that could be used by departed employees to hinder an application/system.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

020.308 Out-Processing / Termination of Information Technology Personnel	Current Version: 2.3
020.300 Administrative Security	Review Date: 03/29/2018

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

Any application or services that are not currently housed with the Kentucky Online Gateway (KOG) system must follow agency processes/procedures for appropriate removal of all employee access upon departure from employment.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Form: E-mail Request Form, COT-F084 Form
- Enterprise IT Form: Staff Service Request Form (and COT Entrance/Exit Form), COT-F181 Form
- Enterprise IT Form: Staff Service Request Form, EZ Version, COT-F181EZ Form
- Kentucky Human Resource Information System (KHRIS)
- OHRM Personnel Forms: Exiting Employees (for Supervisors) Checklist
- OHRM Personnel Procedures Handbook: Section 4.1- Disciplinary/Corrective Action
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information